Listing of the Claims:

1. (Original) A method of improving intrusion detection in a computing network, comprising steps of:

defining intrusion suspicion levels for inbound communications destined for a computing device on the computing network; and

using the defined intrusion suspicion levels to determine if a particular inbound communication destined for the computing device should be treated as an intrusion event.

2. (Original) The method according to Claim 1, further comprising steps of:

defining a sensitivity level for filtering intrusion events; and

determining the intrusion suspicion level of the particular inbound communication;

wherein the using step compares the sensitivity level to the determined intrusion suspicion level.

3. (Original) The method according to Claim 2, wherein the determining step further comprises comparing conditions in the computing device to predetermined conditions which signal a potential intrusion.

4. (Original) The method according to Claim 3, wherein the conditions in the computing device comprise contents of the particular inbound communication.

5. (Original) The method according to Claim 4, wherein the conditions in the computing device further comprise a protocol state of a protocol stack which processes the particular inbound communication.

6. (Original) The method according to Claim 1, further comprising the step of taking one or more defensive actions when the using step determines that the particular

inbound communication should be treated as an intrusion event.

7. (Original) The method according to Claim 6, wherein the defensive actions are determined by consulting intrusion detection policy information.

8. (Original) The method according to Claim 6, wherein the intrusion detection policy information is stored in a network-accessible repository.

9. (Original) The method according to Claim 1, wherein the using step further comprises comparing the particular inbound communication to one or more attack signatures.

10. (Original) The method according to Claim 9, wherein at least one of the attack signatures is a class signature representing a class of attacks.

11. (Original) The method according to Claim 9, wherein the attack signatures are specified as conditions in intrusion detection rules, and wherein each of the intrusion detection rules further comprises one or more actions that are to be taken when the using step determines that the particular inbound communication should be treated as an intrusion event.

12. (Original) The method according to Claim 1, wherein the using step operates in the computing device for which the particular inbound communication is destined.

13. (Original) The method according to Claim 12, wherein the using step operates within layer-specific intrusion detection logic executing in a protocol stack running on the computing device.

14. (Original) The method according to Claim 1, wherein the using step operates in a network device which analyzes communications directed to the computing device for

which the particular inbound communication is destined.

15. (Original) The method according to Claim 1, further comprising steps of:

for each of a plurality of potential intrusion events, defining a set of one or more conditions which describe the potential intrusion event;

associating a sensitivity level with each of the sets of conditions; and

determining a suspicion level of the particular inbound communication;

wherein the using step determines that the particular inbound communication should be treated as an intrusion event when conditions pertaining to the particular inbound communication match a selected one of the sets of conditions and the determined suspicion level maps to the sensitivity level associated with the selected set of conditions.

16. (Withdrawn) A method for improving intrusion detection in a computing network, comprising steps of:

classifying an inbound communication destined for a computing device on the computing network as to an intrusion class which is applicable to the inbound communication; and

determining whether the applicable intrusion class has one or more associated intrusion detection policy specifications, and if so, performing actions specified in the one or more associated intrusion detection policy specifications.

17. (Withdrawn) The method according to Claim 16, wherein the actions include writing a record describing the inbound communication to a file, wherein the record includes the applicable intrusion class.

18. (Withdrawn) The method according to Claim 17, wherein the record includes an identification of a code element where the inbound communication was processed.

19. (Withdrawn) The method according to Claim 18, further comprising the step of:

determining, for each of the records of the file, whether the intrusion class and identification of the code element identify a specific attack, and if so, creating an analysis record for the identified specific attack.

20. (Withdrawn) The method according to Claim 18, further comprising the step of:

determining, for each of the records of the file, whether the intrusion class and identification of the code element identify a specific attack, and if not, performing steps of:

locating packet data pertaining to the record;

comparing the located packet data to attack signatures; and

if a matching attack signature is located by the comparing step, creating an analysis record for a specific attack which corresponds to the matching attack signature, and otherwise creating an analysis record for the intrusion class.

21. (Withdrawn) The method according to Claim 16, wherein the classifying step further comprises locating an attack signature which matches the inbound communication, and the determining step further comprises using one or more keywords which are associated with the located attack signature to retrieve the associated intrusion detection policy specifications.

22. (Original) A system for improving intrusion detection in a computing network, comprising:

means for defining intrusion suspicion levels for inbound communications destined for a computing device on the computing network; and

means for using the defined intrusion suspicion levels to determine if a particular inbound communication destined for the computing device should be treated as an intrusion event.

23. (Original) The system according to Claim 22, further comprising:

means for defining a sensitivity level for filtering intrusion events; and

means for determining the intrusion suspicion level of the particular inbound communication;

wherein the means for using the defined intrusion further comprises means for comparing the sensitivity level to the determined intrusion suspicion level.

24. (Original) The system according to Claim 23, wherein the means for determining further comprises means for comparing conditions in the computing device to predetermined conditions which signal a potential intrusion.

25. (Original) The system according to Claim 22, further comprising means for taking one or more defensive actions when the means for using determines that the particular inbound communication should be treated as an intrusion event, wherein the defensive actions are determined by consulting intrusion detection policy information.

26. (Original) The system according to Claim 22, wherein the means for using further comprises means for comparing the particular inbound communication to one or more attack signatures, wherein the attack signatures are specified as conditions in intrusion detection rules, and wherein each of the intrusion detection rules further comprises one or more actions that are to be taken when the means for using determines that the particular inbound communication should be treated as an intrusion event.

27. (Original) The system according to Claim 22, further comprising:

for each of a plurality of potential intrusion events, means for defining a set of one or more conditions which describe the potential intrusion event;

means for associating a sensitivity level with each of the sets of conditions; and

means for determining a suspicion level of the particular inbound communication;

wherein the means for using determines that the particular inbound communication should be treated as an intrusion event when conditions pertaining to the particular inbound communication match a selected one of the sets of conditions

and the determined suspicion level maps to the sensitivity level associated with the selected set of conditions.

28. (Withdrawn) A system for improving intrusion detection in a computing network, comprising:

means for classifying an inbound communication destined for a computing device on the computing network as to an intrusion class which is applicable to the inbound communication; and

means for determining whether the applicable intrusion class has one or more associated intrusion detection policy specifications, and if so, performing actions specified in the one or more associated intrusion detection policy specifications.

29. (Withdrawn) The system according to Claim 28, wherein the actions include writing a record describing the inbound communication to a file, wherein the record includes the applicable intrusion class and an identification of a code element where the inbound communication was processed.

30. (Withdrawn) The system according to Claim 29, further comprising:

means for determining, for each of the records of the file, whether the intrusion class and identification of the code element identify a specific attack, and if so, creating an analysis record for the identified specific attack, and if not, means for:

locating packet data pertaining to the record;

comparing the located packet data to attack signatures; and

if a matching attack signature is located by the means for comparing, creating an analysis record for a specific attack which corresponds to the matching attack signature, and otherwise creating an analysis record for the intrusion class.

31. (Withdrawn) The system according to Claim 28, wherein the means for classifying further comprises means for locating an attack signature which matches the inbound communication, and the means for determining further comprises means for

using one or more keywords which are associated with the located attack signature to retrieve the associated intrusion detection policy specifications.

32. (Original) A computer program product for improving intrusion detection in a computing network, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for defining intrusion suspicion levels for inbound communications destined for a computing device on the computing network; and

computer-readable program code means for using the defined intrusion suspicion levels to determine if a particular inbound communication destined for the computing device should be treated as an intrusion event.

33. (Original) The computer program product according to Claim 32, further comprising:

computer-readable program code means for defining a sensitivity level for filtering intrusion events; and

computer-readable program code means for determining the intrusion suspicion level of the particular inbound communication;

wherein the computer-readable program code means for using compares the sensitivity level to the determined intrusion suspicion level.

34. (Original) The computer program product according to Claim 33, wherein the computer-readable program code means for determining further comprises computer-readable program code means for comparing conditions in the computing device to predetermined conditions which signal a potential intrusion, the conditions in the computing device comprising contents of the particular inbound communication.

35. (Original) The computer program product according to Claim 33, wherein the computer-readable program code means for determining further comprises computer-

readable program code means for comparing conditions in the computing device to predetermined conditions which signal a potential intrusion, the conditions in the computing device comprising contents of the particular inbound communication and a protocol state of a protocol stack which processes the particular inbound communication.

36. (Original) The computer program product according to Claim 32, further comprising computer-readable program code means for taking one or more defensive actions when the computer-readable program code means for using determines that the particular inbound communication should be treated as an intrusion event, wherein the defensive actions are determined by consulting intrusion detection policy information stored in a policy repository.

37. (Original) The computer program product according to Claim 1, wherein the computer-readable program code means for using further comprises computer-readable program code means for comparing the particular inbound communication to one or more attack signatures, wherein at least one of the attack signatures is a class signature representing a class of attacks.

38. (Original) The computer program product according to Claim 32, wherein the computer-readable program code means for using operates in the computing device for which the particular inbound communication is destined.

39. (Original) The computer program product according to Claim 32, wherein the computer-readable program code means for using operates in a network device which analyzes communications directed to the computing device for which the particular inbound communication is destined.

40. (Original) The computer program product according to Claim 32, further comprising:

computer-readable program code means for specifying, for each of a plurality of potential intrusion events, a set of one or more conditions which describe the potential intrusion event;

computer-readable program code means for associating a sensitivity level with each of the sets of conditions; and

computer-readable program code means for determining a suspicion level of the particular inbound communication;

wherein the computer-readable program code means for using determines that the particular inbound communication should be treated as an intrusion event when conditions pertaining to the particular inbound communication match a selected one of the sets of conditions and the determined suspicion level maps to the sensitivity level associated with the selected set of conditions.

41. (Withdrawn) A computer program product for improving intrusion detection in a computing network, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for classifying an inbound communication destined for a computing device on the computing network as to an intrusion class which is applicable to the inbound communication; and

computer-readable program code means for determining whether the applicable intrusion class has one or more associated intrusion detection policy specifications, and if so, performing actions specified in the one or more associated intrusion detection policy specifications.

42. (Withdrawn) The computer program product according to Claim 41, wherein the actions include writing a record describing the inbound communication to a file, wherein the record includes the applicable intrusion class and an identification of a code element where the inbound communication was processed.

43. (Withdrawn) The computer program product according to Claim 42, further

comprising:

computer-readable program code means for determining, for each of the records of the file, whether the intrusion class and identification of the code element identify a specific attack, and if so, computer-readable program code means for creating an analysis record for the identified specific attack, and if not, computer-readable program code means for:

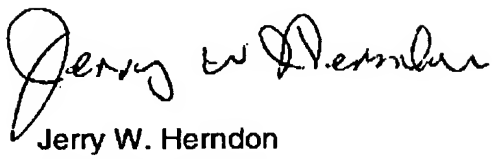
locating packet data pertaining to the record;

comparing the located packet data to attack signatures; and

if a matching attack signature is located by the computer-readable program code means for comparing, creating an analysis record for a specific attack which corresponds to the matching attack signature, and otherwise creating an analysis record for the intrusion class.

44. (Withdrawn) The computer program product according to Claim 41, wherein the computer-readable program code means for classifying further comprises computer-readable program code means for locating an attack signature which matches the inbound communication, and the computer-readable program code means for determining further comprises computer-readable program code means for using one or more keywords which are associated with the located attack signature to retrieve the associated intrusion detection policy specifications.

Respectfully Submitted,



Jerry W. Herndon
Reg. No. 27,901

IBM Docket No. RSW920020011US1
Serial No. 10/058,689
Customer No. 25259
Phone: 919-543-3754
Fax: 919-254-4330